SOLUTION BRIEF

# Ekinops Encryption Solution

## Delivering GDPR Compliant In-flight Data Security Over Any Span

## Background

With ever greater data rates being transported over ever increasing distances, optical transport networks have become a primary target for hackers and other malicious intruders that are looking to steal private data. Transferring data and applications between physical locations means personal and proprietary information is continually on the move and therefore more susceptible to intrusion than when it is not behind the firewall. Communications networks in general are under continual attack from increasingly sophisticated actors making it difficult for service providers and enterprises alike to ensure the safety and security of their data. In fact, most industry surveys show that data security issues rank first among barriers to adoption of next-gen cloud-based services. For the database group the primary concern is server security, protecting the integrity of the data at rest and preventing unauthorized access to corporate information stored inside the data center. The network group has to protect the same data but with the added risk and complexity of doing it while the data is in-flight between locations. This risk is also shared by any network operator that is providing the connectivity service between those locations. In the current regulatory environment, this risk now has greater focus with the implementation of measures such as the General Data Protection Regulation (GDPR) instituted by the European Union that significantly increases both the burden and financial consequences not only of non-compliance but also of any security breach in a compliant network. Ekinops encryption solutions help service providers and other network operators answer the question of how best to comply with regulatory guidelines and minimize potential risk in their networks.

## Do You Know Where Your Data Is?

Most records are kept electronically these days and sensitive information including names, addresses, dates of birth, tax identification numbers, credit card and bank account numbers and medical records are stored on computers and servers where they are increasingly at risk of being stolen; and with more and more data being moved to the Cloud, a single security breach can now potentially expose hundreds of millions of records and there are thousands of security breaches every year. Yet despite the fact that over one-quarter of enterprises globally experienced a data breach in 2019, fewer than one-third report having adopted encryption tools to prevent them[1].

(1) *2020 Thales Data Threat Report, Global Edition*

## The New Regulatory Environment

To address these security issues, the European Union (EU) has developed the GDPR as a new security requirement effective May 25, 2018 in all of its countries. Given its regulatory requirements, GDPR is one of the most impactful developments in network security ever to occur.

One of the key objectives of GDPR is to provide a uniform code for data protection. Though intended to protect private citizens, it has global impact with effects that extend beyond EU, as set forth in the regulation "In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.,"[(2)] which, in this global economy, is virtually any company that does business over the worldwide web.

This burden of protecting the data has a direct impact on network operators as they will be liable for any security breaches while the data is in transit over their networks. The most relevant provision is the concept of "Privacy by Design" which mandates building privacy into the design, operation and management of any system, business process or design specification. Because of their central function to data movement, optical transport networks are an integral part of virtually all network operator systems, processes and designs and, like any other IT or communications sector, can be vulnerable to security compromise. These compromises take the form of either unauthorized access to management systems or—since fiber networks are physical things—taps placed on the optical fiber itself to collect data while it's in transit.

Transport networks also make an obvious target since they operate at Layer 1 of the protocol stack over which all other services ride making them a one-stop-shopping destination for more lucrative Layer 2 and Layer 3 data. With the penalties for a breach of GDPR regulations reaching €20 million or 4% of annual sales, whichever is greater, service providers and other network operator organizations large and small are highly incented to provide the safest and most secure network possible.

## The Ekinops Solution

EKINOPS PM CRYPTO encryption solution is a hardware-based cryptography engine that provides wire speed performance using field-proven industry standard methods (Figure 1). PM CRYPTO uses the strongest AES-GCM 256 based encryption to provide the highest level of security from end-to-end.


*Figure 1 - EKINOPS PM CRYPTO*

It protects data in-flight across high speed optical networks with a hardware based algorithm that operates at Layer 1 to fully encrypt the payload and guarantee the security of even the most critical data and applications (Figure 2).

*(2) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Article 3, Recital 23*


*Figure 2 - In-flight data encryption*

PM CRYPTO employs the Diffie-Hellman key exchange method to exchange both public and private keys, and allows the user to configure the frequency of the key exchange up to several times per minute to prevent keys from being decoded by brute force computing methods (Figure 3a).

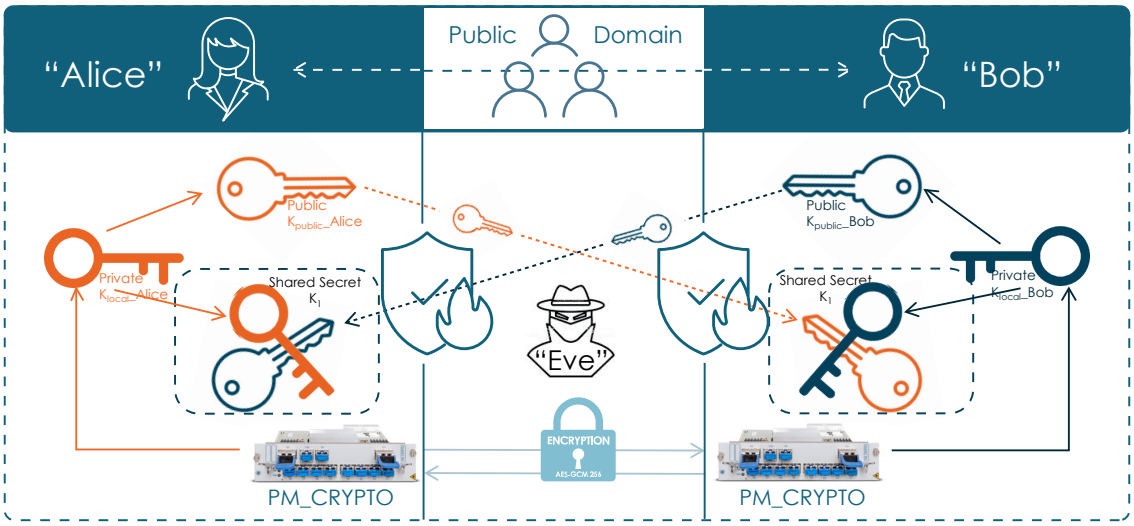


*Figure 3a - Diffie-Hellman key exchange*

It also employs separate keys that enable strong authentication to prevent "man-in-the-middle" type attacks in which a malicious intruder ("Eve") acts as the verified recipient by spoofing their identity to the sender ("Alice" / "Bob") (Figure 3b).

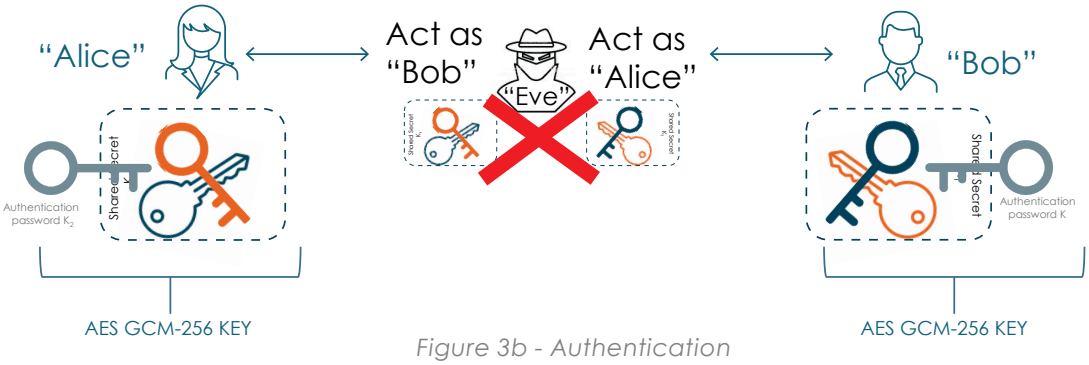


*Figure 3b - Authentication*

As a pluggable module in the Ekinops360 platform, PM CRYPTO can be quickly and easily integrated into any existing or greenfield network simply by connecting either client devices or the line output from existing Ekinops service modules as client interfaces to PM CRYPTO. In this manner, operators can bring their networks into regulatory compliance in the shortest amount of time and with the least cost possible and with the strongest encryption capability available. Operating at Layer 1, it provides bulk encryption

without the penalties imposed by a higher layer solution such as IPSec that encrypts every single packet. The additional overhead created using this approach causes up to a 60% increase in the required data rate which results in significant latency across the network.

Multiprotocol support means service providers can encrypt any service type including 10GbE 4G/8G/10G/16G Fibre Channel, OC-192/STM-64, OTU2/OTU2e in any combination. With the ability to also support 100GbE, service providers need only a single module for all their transport encryption needs to help reduce sparing costs and minimize staff training requirements. With this multi-protocol/multi-rate support, PM CRYPTO makes it easy to offer encryption services with ironclad SLAs to create new high premium revenue streams.

A key differentiator of PM CRYPTO is that it provides what is known as "always on" encryption that eliminates the possibility of data being sent in the clear (i.e., unencrypted). Solutions that offer the possibility of turning encryption off on a port-by-port basis might appear to give the operator greater control, but in reality they introduce the possibility of human error and exposing data to the potential risk of being compromised, a risk that service providers can ill afford to assume.

PM CRYPTO also provides the basis for the most scalable optical transport encryption solution possible. Compared to alternate solutions where the encryption engine resides on the same Digital Signal Processor (DSP) that performs the coherent modulation and detection, PM CRYPTO resides on Ekinops' patented T-Chip processor that encrypts the multiplexed signal before it reaches the DSP. This means new services can be easily added to the encryption engine on a port-by-port or service-by-service basis over a wavelength that has already been commissioned, tested and qualified. This approach eliminates the time and expense of having to deploy a new line card each time a new service is added.

## Key Management

Managing the encryption keys is as important as the encryption itself. Without strong key management controls, the entire process is open to risk of compromise. Using EKINOPS Celestis NMS advanced network management system, the managed services customer retains complete control over key management. Access to encryption management functions within Celestis NMS is partitioned from management of the network elements and services. It requires separate login credentials that are assigned to and controlled by the managed services customer. Authorized users can be assigned as Crypto Officers or Crypto Users for multi-tier access and control. Crypto Officers and Crypto Users can variously control the monitoring, configuration, key exchange and password management of the encrypted services through a dedicated tab on the Celestis NMS panel (see Figure 4).

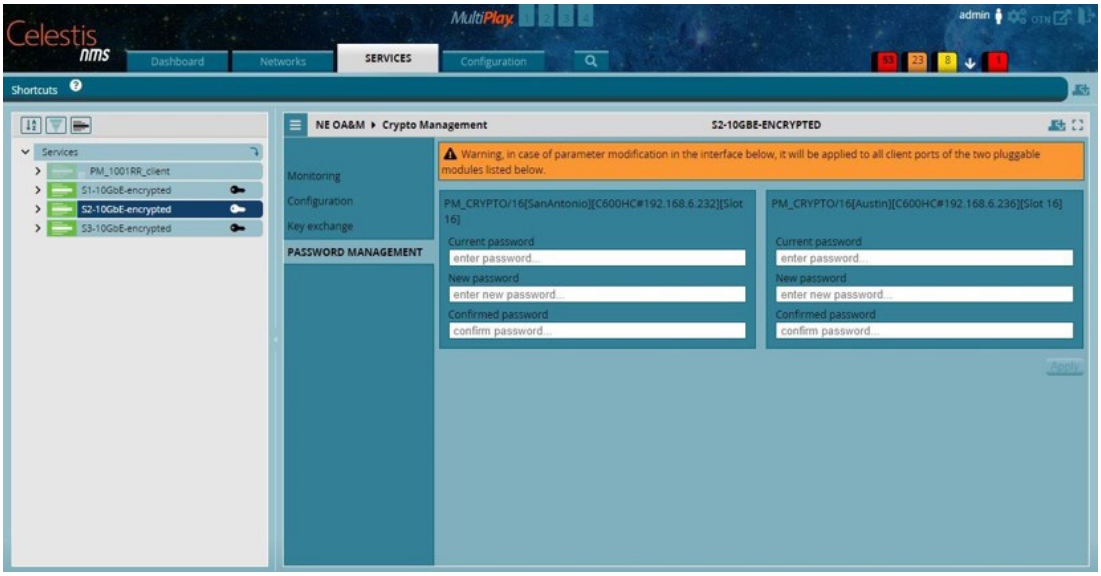


*Figure 4 - Celestis NMS Crypto management*

## Use Case 1: Adding Encryption to an Ekinops Network

PM CRYPTO can be deployed on any Ekinops line system—new or existing—by pairing it with our FlexRate™ modules. In this configuration, the PM CRYPTO acts as a client card for either a 100G client or up top ten 8G/10G/16G services, and encrypting the composite 100G signal before it is handed off to the FlexRate module that then delivers the encrypted channel over a coherent high-speed wavelength (Figure 5). This wavelength can then be combined with other optical channels, both encrypted and non-encrypted alike, on the optical mux or ROADM and transported to any point on the network, whether that point is across town, across the country or even across the ocean.

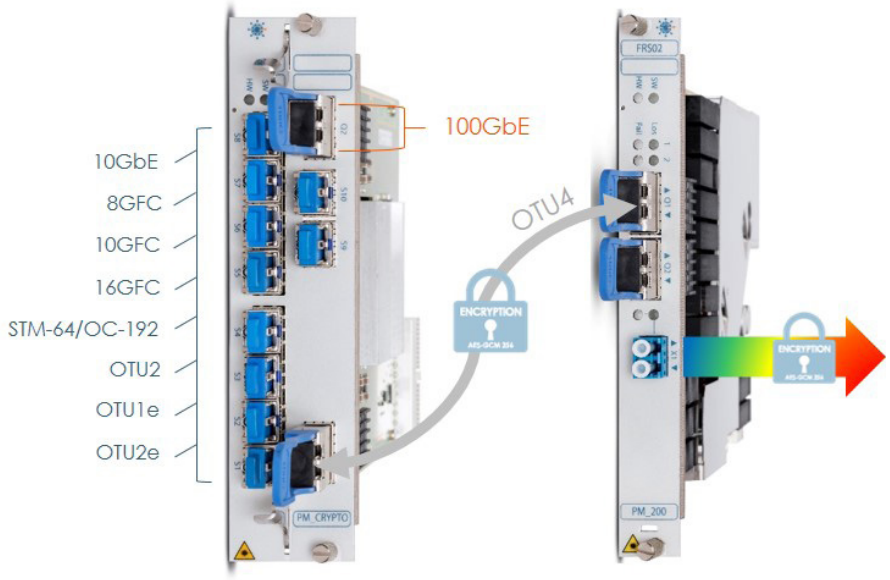


*Figure 5 - Encrypted service transport over FlexRate™ coherent wavelength*

## Use Case 2: Adding Encryption as an Alien Wavelength over an Existing Line System

In addition to operating over an Ekinops network, PM CRYPTO can be just as easily deployed over an existing network that consists of a line system—optical multiplexers, ROADMs and amplifiers—from a vendor other than Ekinops. In this case, the FlexRate module can be directly interconnected with the third-party optical multiplexer as what is termed an "alien wavelength" (Figure 6). In this use case, the network operator can still take advantage of the performance not only of the PM CRYPTO, but also of Ekinops cost-efficient FlexRate transport technology with advanced modulation and coherent detection schemes that can be optimized to reach any distance up to 10,000 Km.

As an alien wavelength, it operates and is managed completely separate from the existing wavelengths so the encrypted link cannot be accessed from the third party management system.

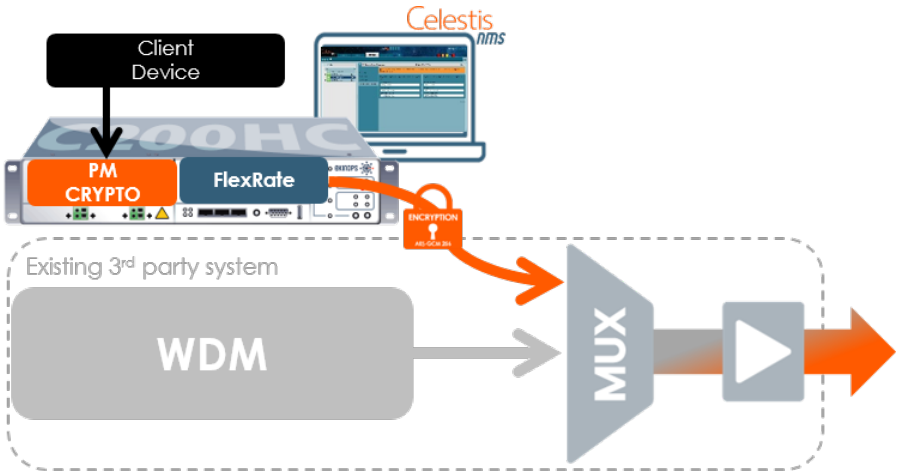


*Figure 6 - Adding encryption over an existing line system*

## Conclusion

Data security is one of the most critical issues in the network today. As more and more sensitive data is stored, processed and transferred electronically, the potential for its compromise increases. Over one-quarter of enterprises globally have data breaches each year exposing billions of records—including names, addresses, credit cards and medical records—with no vertical immune from those malicious actors intent on stealing data, yet fewer than one-third employ any type of encryption. Governments are now reacting to protect the data of private citizens by requiring strict security mechanisms and procedures. Regulations such as GDPR in the EU also impose significant financial penalties for those that do not comply or allow data breaches to occur.

Data is most at risk when it is "in-flight" over the wide area network and outside the corporate firewall. To ensure data security, service providers need an efficient method of encrypting network traffic. Layer 2 and Layer 3 encryption methods such as MACSec and IPSec add latency along with substantial overhead that serves to throttle the throughput of critical data.

EKINOPS PM CRYPTO provides a bulk Layer 1 encryption mechanism based on industry-standard AES-GCM 256 technology that is capable of encrypting an entire high speed transmission frame such as OTU4 that can carry up to 100Gbps of traffic in a single payload consisting of thousands of services. Diffie-Hellman key exchange methodology prevents "man-in-the-middle" attacks and frequent key rotation intervals eliminate brute force decoding attempts.

PM CRYPTO is plug-and-play encryption tool that simplifies the introduction and lowers the cost of securing customer data across the service provider network. Its modular nature means PM CRYPTO can be deployed in any network architecture giving service providers multiple options for adding encryption to their transport network, whether as a new wavelength on an existing Ekinops line system or as an alien wavelength over a third-party line system. With its standards-based G.709 OTU4 output, PM CRYPTO can also be connected to an existing OTN network directly as a client service without the need for a separate transponder and with no impact on the existing line system.

## About Ekinops

Ekinops is a leading provider of open, trusted and innovative network connectivity solutions to service providers around the world. Our programmable and highly scalable solutions enable the fast, flexible, and cost-effective deployment of new services for both high-speed, high-capacity optical transport as well as virtualization-enabled managed enterprise services.

Our product portfolio consists of three highly complementary product and service sets: Ekinops360, OneAccess and Compose.

- Ekinops360 provides optical transport solutions for metro, regional and long-distance networks with WDM for high-capacity point-to-point, ring, and optical mesh architectures, and OTN for improved bandwidth utilization and efficient multi-service aggregation.
- OneAccess offers a wide choice of physical and virtualized deployment options for Layer 2 and Layer 3 access network functions.
- Compose supports service providers in making their networks software-defined with a variety of software management tools and services, including the scalable SD-WAN Xpress and SixSq Edge-to-Cloud solutions.

As service providers embrace SDN and NFV deployment models, Ekinops enables future-proofed deployment today, enabling operators to seamlessly migrate to an open, virtualized delivery model at a time of their choosing.

A global organization, Ekinops (EKI) - a public company traded on the Euronext Paris exchange operates on four continents.

## Contact us

**sales.eu@ekinops.com | sales.asia@ekinops.com | sales.us@ekinops.com | www.ekinops.com**